CLAIMS:

1. A domain manager device for managing a network comprising a plurality of devices, comprising authentication means for issuing to a new device joining the network a predetermined number of symmetric authentication keys, each respective authentication key allowing authenticated communication with one respective other device comprised in the network.

2. The device of claim 1, the authentication means being arranged for generating a predetermined number of authentication tickets, each respective authentication ticket allowing a device with a first identifier to authenticate itself to a device with a second identifier, and for issuing to the new device those authentication tickets whose first identifier matches an identifier for the new device.

3. The device of claim 1, comprising key management means for generating a predetermined number of master device keys and the authentication means being arranged for issuing one of the generated master device keys to the new device.

4. The device of claim 2 and 3, each respective authentication ticket being at least partially encrypted with a master device key from the predetermined number that is associated with the second identifier.

5. The device of claim 3, the key management means being arranged for associating each generated master device key with a mutually unique identifier, assigning to the new device as a device identifier the unique identifier associated with the master device key issued to the new device, and upon the new device ceasing to be part of the network, generating a new master device key and associating the generated new master device key with the unique identifier assigned previously as the device identifier to the new device.

6. The device of claim 4 and 5, the authentication means being arranged for, upon the key management means detecting that the device identifier assigned to the new device was previously assigned to another device,
issuing a set of replacement authentication tickets to the new device, each respective replacement authentication ticket allowing a device with a first identifier to authenticate itself to the new device and being at least partially encrypted with the master device key associated with the first identifier.

7. The device of claim 3, the key management means being arranged for receiving a global revocation list identifying a number of revoked devices,
creating a local revocation list identifying those revoked devices that are comprised in the network, and
generating a number of revocation authentication codes, each respective revocation authentication code enabling authentication of the local revocation list using a respective master device key from the generated predetermined number of master device keys.

8. The device of claim 7, the key management means being arranged for generating each respective revocation authentication code by computing a respective keyed message authentication code of the local revocation list using each respective master device key.

9. The device of claim 1, the predetermined number of authentication keys being chosen as one less than or as equal to or more than a maximum number of devices that may concurrently be comprised in the network.

10. The device of claim 3, the number of master device keys in the set being chosen as equal to or more than a maximum number of devices that may concurrently be comprised in the network.

11. The device of claim 2 and 5, the authentication means being arranged for generating for a particular identifier associated with a particular generated master device key a number of authentication tickets, each generated authentication ticket allowing a device with said particular identifier to authenticate itself to a device with one other of the unique identifiers associated with one of the generated master device keys.

12. A first device arranged to communicate with a second device via a network comprising a plurality of devices, the first device comprising
networking means for requesting to a domain manager device to join the network and for receiving a predetermined number of symmetric authentication keys, each respective authentication key allowing authenticated communication with one respective other device comprised in the network, and
authentication means for communicating with the second device using the symmetric authentication key allowing authenticated communication with the second device.

13. The first device of claim 12, the networking means being arranged for receiving a set of authentication tickets from the domain manager device, each respective ticket allowing the first device to authenticate itself to a respective device from the plurality of devices, and the authentication means being arranged for distributing to the second device the authentication ticket from the set allowing the first device to authenticate itself to the second device.

14. The first device of claim 13, the networking means being arranged for receiving from the second device a further authentication ticket, and
the authentication means being arranged to authenticate the second device upon accepting the received further authentication ticket as valid.

15. The first device of claim 14, the networking means being arranged for further receiving from the domain manager device a master device key, and the authentication means being arranged to accept the received further authentication ticket as valid if the received further authentication ticket can be successfully decrypted using the master device key.

16. The first device of claim 14 or 15, the authentication means being arranged for deriving a session key from information contained in the distributed ticket and in the received further authentication ticket.

17. The first device of claim 15, the further authentication ticket being encrypted, and the authentication means being arranged to, upon failing to decrypt the further authentication ticket with the master device key, distributing to the second device a new

authentication ticket allowing the second device to authenticate itself to the first device, the new authentication ticket being at least partially encrypted with the master device key of the second device.

18. The first device of claim 15, the authentication means being arranged for receiving from the second device a new ticket allowing the first device to authenticate itself to the second device, the new ticket being at least partially encrypted with the master device key of the first device,
and for decrypting the new ticket with the master device key and for replacing the ticket from the set allowing the first device to authenticate itself to the second device by the new ticket upon successful decryption of the new ticket.

19. The first device of claim 15, the networking means being arranged for receiving a local revocation list identifying revoked devices that are comprised in the network and a number of revocation authentication codes, each respective revocation authentication code enabling authentication of the local revocation list using a respective master device key,
the authentication means being arranged for accepting the local revocation list as valid if one of the received revocation authentication codes can be successfully decrypted using the master device key.

20. A computer program product arranged to cause a device to operate as the device of claim 1.

21. A computer program product arranged to cause a device to operate as the device of claim 12.